State of Indiana Policy and Standards

OneDrive for Business

Standard ID

IOT-CS-OPS-001

Published Date

11/1/2016

Effective Date

11/1/2016

Last Updated

10/31/2016

Next Review Date

10/31/2017

Policy

23.0 Operational Policies
23.3 Delivery Services
23.3.1 Delivery Services

Purpose

The Indiana Office of Technology (IOT) has purchased SharePoint Online subscription services for a number of agencies. One element of this subscription is OneDrive for Business. Adherence to this policy shall be used by agencies currently utilizing OneDrive for Business.

Scope

IOT Supported Entities

Statement

Agencies and agency personnel shall not store Personally Identifiable Information (PII), Personal Health Information (PHI), or otherwise confidential information in OneDrive for Business. Confidential data accessed by unauthorized entities could cause personal or institutional financial loss, or constitute a violation of a statute, act, or law.

When an employee leaves an agency, the manager or agency has 30 days to retrieve said employee's data from OneDrive for Business.

Agencies shall review sharing privileges quarterly and remove privileges when they are no longer needed.

Agencies shall notify IOT if they believe security patches may interfere with OneDrive for Business.

IOT shall disable OneDrive for Business at any time if it is determined that the tool has been compromised or cannot comply with security requirements defined by IOT's security standards.

Employees’ OneDrive for Business shall not be used for permanent storage of public records or confidential data.

OneDrive for Business does not get backed up by IOT, therefore restores of data are not available.

For governmental entities utilizing the OneDrive for Business services of IOT, it remains the responsibility of the governmental entity to manage their records and comply with applicable laws, policies, and retention schedules.

Roles

All Personnel

IOT Personnel

Responsibilities

All personnel shall manage information according to agency record and retentions policies set by the IARA.

Management Commitment

Management shall ensure that all personnel are trained and aware of requirements related to use of OneDrive for Business.

Coordination Among Organizational Entities

Agencies shall coordinate with IOT for security patch exceptions. IOT will communicate if at any point the system will be disabled due to maintenance or a security issue.

Compliance

Agencies shall review access quarterly and remove users based on the least privilege security standard statements. Any PII, PHI, or other confidential information found to be stored in OneDrive for Business shall be reported to the Agency Head and the State's CISO.

Exceptions

Exception requests can be submitted for patching, otherwise all other statements are required.

Associated Documents

OneDrive for Business